anchore

CASE STUDY

Lark uses Anchore Enterprise to control Container Sprawl and Reduce CVEs

Lark extends the concepts of smart health and lifestyle hacking beyond a traditional consumer fitness tracker to significantly improve patient outcomes in clinical medicine. By combining smart, connected-health devices with a powerful artificial intelligence (AI) platform, Lark provides personalized, interactive health coaching for pre-diabetes and hypertension patients. The health tech market, mostly having to maintain compliance, temper Lark's need for agility. Alongside the usual challenges of creating a superlative product, medical startups also have to operate within a harsh regulatory environment, with long lead-times to market and some of the highest testing and security standards.

In the United States, state and federal regulations govern medical products. Health Tech firms such as Lark must consider The Health Insurance Portability and Accountability Act (HIPAA) at every development stage. Failure to comply with HIPAA is a serious offense, carrying a maximum of a $50,000 fine per violation. In 2019, the average cost of a data breach in the US medical industry was $6.45 million.

For health tech startups, a security breach can be an existential threat. Even without the risk of substantial fines, the public views medical data as being sacrosanct. Losing any medical data risks irrecoverable reputational impact.

LARK HEALTH AT A GLANCE

Mountain View, CA | www.lark.com | Health/Health Tech

CHALLENGES

- An explosion of containers and tags
- Each additional container and tag had the possibility of introducing new common vulnerabilities and exposures (CVEs) and security issues into their system, either from a directly installed application.
- Scanning Lark images in production

SOLUTIONS

- Implement Anchore Enterprise in Passive Analysis Trigger Mode in their development environment to allow continuous container deployment and. scanning of only the images in production.

RESULTS

- Utilizing Anchore, Lark was able to replace a manual and labor-intensive task with an automated, developer-friendly workflow.
- With Anchore Enterprise and its reporting, the company connected the security team to the application development lifecycle without burdening them with additional manual work or slowing down development.

Challenge

Lark faced a common problem many container-first development teams face: an explosion of both containers and container tags to manage.

Most container workflows will naturally produce a constant stream of new containers. After passing through a CI pipeline, it is common practice for every application or service to have a container created, tagged, and then pushed to a container repository. They exacerbate this challenge in platforms that have adopted a microservices pattern, where many components contribute to the overall scale and pace of container sprawl.

The judicious use of automated life cycle policies (where these exist) can reduce container sprawl. However, it is still commonplace for companies to have hundreds, if not thousands, of images and tags.

For Lark, the real problem was that each additional container and tag had the possibility of introducing new common vulnerabilities and exposures (CVEs) and security issues into their system, either from a directly installed application dependency or from an inherited base container.

"With Anchore Enterprise and its powerful reporting, Lark connected their security team to the application development lifecycle without burdening them with additional manual work or slowing down development."

Solution

The team's approach to implementing Anchore was to minimize the disruption of introducing a new tool. Rather than re-writing the many CI/CD pipelines in use at Lark, Tyler took the approach of leveraging the Kubernetes admission controller together with a tiered approach to policies, getting more permissive with each step further left:

- Production: The DevOps team implements Anchore in production to scan all images in production. Anchore provides reports of the vulnerabilities that are in production allowing the Security and Eng teams to review and remediate them.

Results

With Anchore Enterprise and its powerful reporting, Lark connected their security team to the application development lifecycle without burdening them with additional manual work or slowing down development.

Anchore has allowed Lark to substantially increase visibility into potential security issues without requiring massive amounts of operational effort. It is integrated into existing workflows without necessitating a change of procedures and offered valuable insights into how containers are being used.

> ***"By adopting a graduated application of modes, the Lark DevOps team could guarantee Lark's platform's operational safety while ensuring that development cadence was uninterrupted."***

About Anchore

Based out of Santa Barbara, California and Northern Virginia, Anchore provides a set of tools that provide visibility, transparency and control of your container environment. Anchore aims to secure container workloads at scale without impacting deployment velocity. Our Anchore Professional Services team helps users leverage Anchore to analyze, inspect, scan and apply custom policies to container images within custom CI/CD pipelines.

anchore

info@anchore.com

anchore.com